Annexe 1.1

Contrat d'utilisation des données Infrastructure de base Bibliothèque numérique

PARTIE 1 : GÉNÉRALITÉS 2

1. Contexte 2

2. Définitions 3

3. Organisation de la sécurité de l'information 3

3.1 Politique de sécurité de l'information et délégué à la protection des données 3

3.2 Plan de gestion des fuites de données 4

3.3 Traitement des fuites de données 4

3.4 Demandes de l'autorité de contrôle 4

3.5 Demandes des personnes concernées 4

3.6 Documentation 5

4. Informations générales concernant le traitement des données à caractère personnel 5

4.1 Catégories de personnes concernées 5

4.2 Catégories de données à caractère personnel 5

4.3 Lieu où les données à caractère personnel sont conservées 5

4.4 Mesures de sécurité 6

4.5 Lien avec le registre national 8

4.6 Développements futurs et liens 9

4.7 Personnes de contact 10

4.7.1 Délégué à la protection des données 10

4.7.2 Coordonnées en cas de fuite de données 10

5. Données spécifiques concernant la communication unique dans le cadre de l'adhésion de la VGC au système bibliothécaire unifié 10

5.1 Objet de la communication 10

5.2 Finalités et base juridique 11

PARTIE 2 : UTILISATION DES DONNÉES 13

1. Utilisation et traitement autorisés des données à caractère personnel 13

2. Obligations de la VGC 13
2.1 Généralités 13
2.2 Responsabilité envers ses propres collaborateurs 14
2.3 Communication depuis le système de bibliothèque 15
2.3.1 Communication fonctionnelle 15
2.3.2 Module marketing 15
2.4 Rapports et statistiques 15
2.5 Information des utilisateurs finaux 16
2.6 Assistance en cas de fuites de données 16
2.7 Assistance en cas de demandes de l'autorité de contrôle 17
2.8 Assistance en cas de demandes émanant des personnes concernées 17
3. Contrôle 17
PARTIE 3 : HORS CHAMP D'APPLICATION 18
1. Marketing direct personnalisé 18
2. Traitement propre en tant que responsable du traitement en dehors du cadre de l'infrastructure de base de la bibliothèque numérique 18

PARTIE 1 : GÉNÉRALITÉS

1. Contexte

L'infrastructure de base de la bibliothèque numérique vise à :

- Faciliter, uniformiser et rendre plus efficaces les processus de travail administratifs des bibliothèques publiques grâce à une approche supralocale dans un système bibliothécaire unifié ;
- Offrir un fichier unique d'emprunteurs dans lequel chaque emprunteur n'apparaît qu'une seule fois et où les données sont à tout moment à jour ;
- d'améliorer le service aux utilisateurs finaux grâce à une approche supralocale dans des sites web de bibliothèques unifiés, optimisés et optimisables pour le site web, le catalogue et les services « Ma bibliothèque » de la bibliothèque.

En ce qui concerne l'objet de l'accord sur l'infrastructure de base de la bibliothèque numérique (ci-après dénommé « l'accord »), la VGC accepte que Cultuurconnect agisse en tant que responsable du traitement au sens de la législation sur la protection de la vie privée et qu'elle agisse elle-même en tant qu'utilisateur.

La qualification de la VGC s'étend aux bibliothèques publiques néerlandophones de la Région de Bruxelles-Capitale qui sont reliées à l'infrastructure de base de la bibliothèque numérique. La VGC inclura les dispositions nécessaires à cet égard dans ses relations avec les communes concernées, afin que toutes les dispositions, droits/possibilités,

responsabilités et obligations figurant dans la présente annexe s'appliquent également aux communes concernées.

En tant que responsable du traitement, Cultuurconnect a passé des marchés et conclu des contrats avec les prestataires de services informatiques de l'infrastructure de base de la bibliothèque numérique (voir l'article 1, paragraphe 3, de la convention), en fonction de son développement et de sa gestion. Ces prestataires de services informatiques sont des sous-traitants en ce qui concerne le traitement des données à caractère personnel dans le cadre des contrats concernés, et Cultuurconnect conclut des contrats de sous-traitance avec les prestataires de services informatiques concernés. Ces contrats de sous-traitance sont établis sur la base du système des « mesures de référence pour la sécurité de tout traitement de données à caractère personnel » de la Commission de la protection de la vie privée (aujourd'hui : Autorité de protection des données).

La VGC accepte de n'agir en matière de traitement des données à caractère personnel que conformément à l'accord et à la présente annexe.

Le groupe de pilotage Infrastructure de base Bibliothèque numérique, au sein duquel le secteur des bibliothèques publiques est représenté (voir l'article 3 de l'accord), est également impliqué dans les questions liées à la protection de la vie privée, mais n'intervient pas dans ce domaine compte tenu de la responsabilité de Cultuurconnect en tant que sous-traitant.

Les modifications apportées à la présente annexe par Cultuurconnect sont communiquées à la VGC par courrier et/ou par e-mail. La date d'envoi correspond à la date de notification. Si la VGC n'approuve pas la modification proposée, elle a le droit de résilier le Contrat par lettre recommandée, sauf si la modification a pour but de mettre la présente Annexe en conformité avec des lois et règlements contraignants modifiés. Cette résiliation doit intervenir dans les 3 mois suivant la notification de la modification, la date d'envoi de la lettre recommandée étant considérée comme la date de résiliation.

2. Définitions

La présente Annexe utilise les mêmes définitions que celles utilisées dans les lois et réglementations applicables en matière de traitement des données à caractère personnel, y compris, en tout état de cause, le Règlement général sur la protection des données (RGPD).

3. Organisation de l' e sécurité de l'information

3.1 Politique de sécurité de l'information et délégué à la protection des données

Dans le cadre de la mise en place de l'infrastructure de base de la bibliothèque numérique, Cultuurconnect applique des normes strictes en matière de droits d'utilisation et de confidentialité des utilisateurs finaux, de responsabilité sociale et de respect d'un climat de coopération fondé sur l'ouverture et la transparence.

Cultuurconnect applique une politique écrite en matière de sécurité de l'information, qui décrit les stratégies et les mesures retenues pour la sécurité des données, et la met à jour périodiquement sur la base d'évaluations. Cultuurconnect met en œuvre les mesures de sécurité techniques et organisationnelles appropriées, comme l'exige l'article 32 du RGPD.

Cultuurconnect dispose d'un délégué à la protection des données qui répond aux exigences du RGPD.

Cultuurconnect conclut des déclarations sur l'honneur avec tous les collaborateurs qui, dans le cadre de l'exercice de leurs fonctions, doivent avoir accès à des données à caractère personnel, afin qu'ils s'engagent à n'utiliser cet accès que dans le cadre strict de l'exercice de leurs fonctions.

3.2 Plan de gestion des fuites de données

Cultuurconnect dispose d'un plan de gestion en cas d'incidents de sécurité compromettant la disponibilité, l'intégrité et/ou la confidentialité des données à caractère personnel (violation des données à caractère personnel, voir art. 4 du RGPD). Cette procédure décrit les mesures à prendre en cas de découverte d'une fuite de données, ainsi que les personnes responsables de la gestion de cet incident et du rétablissement d'une situation saine.

Cultuurconnect tient un registre des fuites de données.

3.3 Traitement des fuites de données

En cas de fuite de données, Cultuurconnect se conformera aux obligations légales en la matière.

Cultuurconnect signalera les fuites de données à la VGC dans les plus brefs délais. La notification des fuites de données soumises à une obligation légale de déclaration sera adressée à la personne de contact de la VGC mentionnée au point 4.7.2. Cette notification sera effectuée au plus tard 48 heures après en avoir pris connaissance et comprendra, dans la mesure où ces informations sont connues : (a) la nature de l'incident ; (b) la date et l'heure auxquelles l'incident s'est produit et a été découvert ; (c) le nombre de personnes concernées par l'incident ; (d) les catégories de données à caractère personnel concernées ; (e) les mesures prises pour remédier à l'incident, telles que le cryptage ou d'autres mesures techniques ou organisationnelles, y compris les mesures visant à limiter les conséquences négatives éventuelles ; (f) le nom et les coordonnées du délégué à la protection des données ou d'une autre personne de contact ; et (g) une description des conséquences probables de l'incident.

3.4 Demandes de l'autorité de contrôle

Cultuurconnect répondra aux demandes de l'autorité de contrôle et donnera suite aux communications, avis ou injonctions éventuels de l'autorité de contrôle, dans les délais spécifiés par celle-ci.

3.5 Demandes des personnes concernées

Les personnes concernées peuvent exercer leurs droits de différentes manières. Tous les droits peuvent être exercés en contactant le délégué à la protection des données de Cultuurconnect, certains droits peuvent être exercés via le profil « Mijn Bibliotheek » (Ma bibliothèque) par la personne concernée elle-même, ou via le guichet de sa propre bibliothèque. Cultuurconnect s'engage à être le point de contact pour toute demande des personnes concernées dans le cadre de l'exercice de leurs droits.

3.6 Documentation

Cultuurconnect conserve et met régulièrement à jour toute la documentation pertinente relative à la sécurité de l'information. Cultuurconnect ne refusera pas sans motif valable une demande d'accès de la VGC concernant le traitement des données à caractère personnel dans le cadre de l'accord.

4. Informations générales concernant le traitement des données à caractère personnel d'

4.1 Catégories de personnes concernées

Utilisateurs finaux des bibliothèques publiques néerlandophones de la Région de Bruxelles-Capitale
Employés des bibliothèques publiques néerlandophones de la Région de Bruxelles-Capitale
Collaborateurs de la VGC Collaborateurs
de Cultuurconnect

4.2 Catégories de données à caractère

personnel Des utilisateurs finaux :

- Données d'identification : nom (le cas échéant, extrait de la carte d'identité électronique) ;
- Coordonnées : résidence principale (le cas échéant, extraite de la carte d'identité électronique), adresse supplémentaire éventuelle (par exemple, adresse professionnelle, adresse de logement étudiant), numéro de téléphone, adresse e-mail ;
- Données de connexion : nom d'utilisateur, mot de passe ;
- Caractéristiques personnelles : sexe, date de naissance (le cas échéant, extraite de la carte d'identité électronique) ;
- Numéro de registre national et/ou INSZ ;
- Données de bibliothèque : numéro de carte de bibliothèque, données d'abonnement, historique des emprunts (ce qui a été emprunté, quand, quand cela a été rendu, ce qui a été réservé), historique des paiements (quels montants sont dus, quels montants ont été payés et quand), historique des messages (quelles lettres ont été reçues) ;
- Données de connexion des activités des utilisateurs, par exemple adresse IP ;
- Préférences de communication : préférence pour la réception de messages, par exemple préférence pour les e-mails ou les lettres, préférence linguistique ;
- Données anonymes ou agrégées dans le cadre de l'utilisation du site web, par exemple type de navigateur, système d'exploitation utilisé, pages visitées ;
- Listes de titres préférés.

Pour les collaborateurs (de la bibliothèque, de la VGC ou de Cultuurconnect) :

- Données d'identification : nom ;
- Coordonnées : adresse e-mail ;
- Données de connexion : nom d'utilisateur, mot de passe ;
- Données relatives à la bibliothèque : bibliothèque ;
- Données de connexion relatives aux opérations de gestion effectuées par les employés.

4.3 Lieu où les données à caractère personnel sont conservées

Toutes les données collectées dans le cadre de l'utilisation de l'infrastructure de base de la bibliothèque numérique sont hébergées dans un lieu externe au sein de l'UE afin de permettre une gestion efficace des systèmes informatiques par les fournisseurs informatiques :

- Les données saisies dans le système de bibliothèque, ainsi que les données de connexion et les données de connexion des employés de la bibliothèque, de la VGC et de Cultuurconnect, sont conservées aux Pays-Bas (avec une reprise après sinistre en Allemagne).

- Les données anonymes ou agrégées et l'adresse IP collectées dans le cadre de l'utilisation du site web de la bibliothèque via des cookies, ainsi que les données de connexion et les données de connexion des employés de la bibliothèque, de la VGC et de Cultuurconnect, sont conservées en Belgique.

- Les données communiquées dans le cadre de l'inscription et de la connexion à Ma Bibliothèque, ainsi que les données de connexion et les données de journalisation des employés de la bibliothèque, de la VGC et de Cultuurconnect, sont conservées en Irlande.

Cultuurconnect prend des mesures raisonnables pour assurer la sauvegarde des données. Cultuurconnect veille à ce que les données à caractère personnel ne soient pas transmises à des tiers, sauf si cela est nécessaire pour le traitement prévu (y compris les possibilités de sauvegarde). La transmission à des pays tiers est expressément interdite, sauf avec l'autorisation expresse de Cultuurconnect et à condition qu'une protection adéquate conforme aux normes du RGPD soit garantie.

4.4 Mesures de sécurité

Cultuurconnect a mis en place de nombreuses mesures de sécurité par le biais des accords de traitement conclus avec les prestataires de services informatiques (voir également ci-dessus, 1). Dans les grandes lignes, celles-ci concernent :

A. Mesures de sécurité physiques

Contrôles physiques et

environnementaux

• Sécurité 24 heures sur 24
• Contrôles visant à empêcher tout accès non autorisé
• Toutes les portes, y compris les cages, sont sécurisées par des « cartes de proximité » et des « lecteurs biométriques de géométrie de la main ».
• Couverture par caméras numériques en circuit fermé (CCTV) de l'ensemble du centre de données, y compris les cages et le système d'archivage
• CCTV intégrée au contrôle d'accès et au système d'alarme
• Capteurs de mouvement reliés à des sources lumineuses et couverture CCTV
• Contrôle et filtrage des marchandises entrantes
• Identification des visiteurs à leur arrivée et accompagnement jusqu'à leur destination au sein du centre de données
• Réception et expédition des marchandises séparées des zones de colocalisation
• Un système CVC pour des conditions optimales en matière de température, de circulation de l'air et d'humidité. Les temps d'arrêt dus à des pannes matérielles sont ainsi réduits au minimum.

Afin de garantir la continuité des services, les mesures suivantes ont été prises pour prévenir, détecter et traiter les menaces physiques telles que les incendies ou les inondations.

• Systèmes de lutte contre l'incendie
• Régulation de l'humidité et de la température

• Plancher surélevé pour permettre une circulation d'air continue
• Connecté à Internet via des liaisons redondantes et diversifiées provenant de plusieurs fournisseurs d'accès Internet, qui sont gérées à partir de plusieurs points de présence du fournisseur de télécommunications.
• Alimentation électrique souterraine pour les services publics
• Systèmes d'alimentation électrique sans coupure (UPS)
• Unités de distribution d'alimentation redondantes (PDU)
• Générateurs diesel avec stockage sur site du carburant diesel à chaque emplacement du centre de données
• Sauvegardes nocturnes des données
• Tests réguliers de restauration des sauvegardes
• Reprise après sinistre

B. Sécurisation des réseaux Mesures de

sécurité dans le centre de données :
• Connexion à Internet via des liaisons redondantes, empruntant différents itinéraires, provenant de divers fournisseurs d'accès Internet de plusieurs opérateurs de télécommunications Points de présence
• Les pare-feu et les routeurs périphériques bloquent les protocoles non autorisés
• Les pare-feu internes séparent le trafic entre les couches application et base de données
• Les équilibreurs de charge fournissent des proxys pour le trafic interne
• Le processeur utilise diverses méthodes pour prévenir, détecter et supprimer les logiciels malveillants
• Des audits de sécurité tiers sont effectués périodiquement
• Les collaborateurs chargés de la sécurité de l'information du sous-traitant surveillent les notifications provenant de diverses sources et les alertes des systèmes internes afin d'identifier et de gérer les menaces
• Chiffrement de la base de données (sur la base d'un planning de développement

prioritaire) Sécurisation du trafic entre le client et le serveur (réseau sécurisé ou

HTTPS). Sécurisation de la connexion avec Mijn Bibliotheek (HTTPS).

Sécurisation des connexions entre le registre national et le système de bibliothèque unifié (voir également 4.5).

C. Sécurité logique

Accès limité et contrôlé (uniquement) pour les collaborateurs autorisés des prestataires informatiques (principe du besoin d'en connaître), avec gestion individuelle des identifiants et mots de passe, et expiration périodique des mots de passe.

Définition claire des rôles des administrateurs ayant accès aux données à caractère personnel (uniquement celles qui sont nécessaires).

- Une bibliothèque ne voit que les données de ses propres clients (abonnement à sa propre bibliothèque ou à un groupe de coopération) ;

- Il est possible de diversifier les rôles des utilisateurs pour les administrateurs, afin que le principe du besoin d'en connaître puisse être respecté autant que possible. Le rôle d'utilisateur d'un administrateur détermine les données que celui-ci peut voir.
- Utilisation de connexions d'administration personnelles avec une autorisation/un rôle d'utilisateur spécifique, pour lesquelles des mots de passe forts sont exigés. La structure obligatoire du mot de passe est configurable dans le système. L'objectif est de rendre la date d'expiration du mot de passe configurable pour le système à terme (voir également la PARTIE 2, 2.2 ci-dessous).

Enregistrement et connexion sécurisés et éclairés des utilisateurs finaux avec un mot de passe choisi par eux-mêmes, avec contrôle de sécurité et déconnexion automatique.

D. Journalisation

Le système dispose d'une fonctionnalité de journalisation étendue. Cette fonctionnalité permet, dans certains cas, de retrouver des informations relatives à l'accès aux données à caractère personnel (quelles données à caractère personnel, par qui, quand, quelle action) afin de détecter tout accès non autorisé et tout autre traitement.

Les recherches effectuées sur les données à caractère personnel (journal d'audit) sont conservées suffisamment longtemps (au moins 6 mois en ligne et 10 ans hors ligne) afin de permettre un contrôle plus efficace. L'accès à ces journaux d'audit est réservé aux collaborateurs autorisés de Cultuurconnect.

4.5 Lien avec le registre national

Cultuurconnect a obtenu deux autorisations générales pour le secteur des bibliothèques publiques en Flandre et à Bruxelles. Les communes peuvent démontrer, par le biais d'une demande individuelle, qu'elles remplissent les conditions énumérées dans l'autorisation générale afin de pouvoir effectuer le traitement des données qui y est décrit. Il s'agit de :
- Délibération RR n° 28/2009 du 18 mai 2009 : demande de Bibnet au nom des bibliothèques publiques néerlandophones de Flandre et de Bruxelles visant à obtenir l'accès aux données d'information du Registre national pour l'identification et la gestion de leurs membres (RN/MA/2009/013) ;
- Délibération n° 18/020 du 6 février 2018 relative à l'accès aux registres de la Banque-Carrefour par les bibliothèques publiques néerlandophones de Flandre et de Bruxelles à des fins d'identification et de gestion de leurs membres (question de l'asbl Cultuurconnect).

Ces autorisations générales donnent aux communes/bibliothèques qui ont introduit une demande approuvée (et tant qu'elles remplissent les conditions imposées) le droit, dans le cadre de l'identification et de la gestion de leurs membres :
- accéder à certaines informations contenues dans le Registre national, à savoir celles mentionnées à l'article 3, paragraphe 1, 1°, 2° et 5°, de la loi sur le Registre national : le nom, les prénoms, la date de naissance et le lieu de résidence principal des personnes concernées ;
- utiliser le numéro d'identification du Registre national ;
- accéder aux mêmes données à caractère personnel issues des registres de la Banque-Carrefour (nom, prénoms, date de naissance et résidence principale) ;

- utiliser le numéro d'identification attribué par la Banque-Carrefour de la sécurité sociale (cette utilisation est libre sur la base de l'article 8, paragraphe 2, de la loi du 15 janvier 1990 portant création et organisation d'une Banque-Carrefour de la sécurité sociale.

Les communes/bibliothèques qui, au moment de la signature de la convention, ne disposeraient pas encore d'une autorisation individuelle, s'engagent à entamer la procédure de demande dans les plus brefs délais et à tout mettre en œuvre pour obtenir l'autorisation individuelle.
Les communes peuvent introduire une demande dans le cadre de l'autorisation générale à l'aide des formulaires et de l'adresse de contact disponibles sur le site web de l'Autorité de protection des données.

Cultuurconnect assure la connexion technique entre le système de bibliothèque et le RR/KSZ afin de garantir l'exactitude et la mise à jour des données de l'utilisateur final. Cultuurconnect prend à cet effet les mesures techniques adéquates pour empêcher l'accès à des données à caractère personnel autres que celles couvertes par les autorisations.
Pour cette connexion, il est fait appel à l'Agence d'intégration des services de l'information de Flandre (MAGDA). Cette connexion permet une synchronisation continue entre le fichier des emprunteurs du système de bibliothèque et les données du Registre national auxquelles l'accès est accordé, ce qui garantit la mise à jour et l'exactitude permanentes des données dans le fichier des emprunteurs.

Cultuurconnect demandera, dans la mesure du possible et si cela s'avère pertinent, une extension des autorisations (en ce qui concerne les catégories de données à caractère personnel). Cultuurconnect examine cette question en collaboration avec le groupe de pilotage Basisinfrastructuur Digitale Bibliotheek (Infrastructure de base de la bibliothèque numérique).

4.6 Développements futurs et liens

Cultuurconnect souhaite maintenir l'infrastructure de base de la bibliothèque numérique efficace, pertinente et à jour et, si nécessaire ou souhaitable, mettra en place des développements et/ou des liens avec d'autres systèmes, notamment en vue de :

- adapter les services fournis dans le cadre du Contrat aux évolutions et tendances (technologiques) actuelles,
- des objectifs culturels supralocaux,
- la poursuite de l'innovation dans la politique culturelle locale,
- les modifications du cadre législatif et réglementaire.

En tant que responsable du traitement, Cultuurconnect prendra toujours toutes les mesures appropriées pour protéger les données à caractère personnel.

Ces développements seront toujours discutés au préalable avec le groupe de pilotage Infrastructure de base de la bibliothèque numérique mentionné à l'article 3 de l'accord. Cultuurconnect en informera toujours la VGC en temps utile et avec soin, par courrier et/ou par e-mail. La date d'envoi correspond à la date de notification. Cela peut donner lieu soit à une nouvelle fonctionnalité qui peut être supprimée au choix de la VGC (le cas échéant, un addendum à l'accord, avec éventuellement une modification des tarifs, sera conclu), soit à une intégration qui fait partie intégrante de l'infrastructure de base de la bibliothèque numérique. Dans ce dernier cas, la VGC obtient le droit de résilier le Contrat par lettre recommandée, à moins que l'intégration

a pour objectif de mettre l'infrastructure de base en conformité avec les modifications apportées à la législation et à la réglementation contraignantes. Cette résiliation doit intervenir dans les trois mois suivant la notification de la modification, la date d'envoi de la lettre recommandée faisant foi pour la date de résiliation.

4.7 Personnes de contact

4.7.1 Délégué à la protection des données

Cultuurconnect
dpo@cultuurconnect.be

VGC
dpo@vgc.be

4.7.2 Coordonnées en cas de fuite de données

Cultuurconnect
servicedesk@cultuurconnect.beVGC
dpo@cultuurconnect.be

VGC
dpo@vgc.be

5. Données spécifiques concernant la communication unique dans le cadre du raccordement de la VGC au système de bibliothèque unifié

À la suite du raccordement de la VGC au système de bibliothèques unifié, les données à caractère personnel provenant de l'environnement numérique des bibliothèques/communes sont communiquées une seule fois à Cultuurconnect. Bien que l'ensemble de la présente annexe s'applique à cette communication, un certain nombre d'informations supplémentaires spécifiques à cette communication sont incluses ci-dessous, conformément au décret relatif à la communication électronique de données administratives du 18 juillet 2008 (décret egov ; cf. « protocole » à l'article 8).

5.1 Objet de la communication

Lors du raccordement de la VGC au système bibliothécaire unifié, les données personnelles suivantes, relatives aux membres déjà existants des bibliothèques publiques néerlandophones de la Région de Bruxelles-Capitale avant le raccordement, seront communiquées une seule fois :

- Données d'identification : nom (le cas échéant, lu à partir de la carte d'identité électronique) ;
- Coordonnées : résidence principale (le cas échéant, extraite de la carte d'identité électronique), adresse supplémentaire éventuelle (par exemple, adresse professionnelle, adresse de kot), numéro de téléphone, adresse e-mail ;
- Caractéristiques personnelles : sexe, date de naissance (le cas échéant, extraite de la carte d'identité électronique) ;
- Numéro de registre national et/ou INSZ (si la bibliothèque dispose d'une autorisation) ;
- Données de la bibliothèque : numéro de carte de bibliothèque, données d'abonnement, prêts en cours, paiements et réservations, historique des emprunts (le cas échéant).

La communication s'effectue via le protocole SFTP (Secure File Transfer Protocol). Dans le cadre de la communication, les transactions et les frais d'emprunt en cours remontant jusqu'à 5 ans sont rechargés. Le

L'historique des emprunts est chargé jusqu'à deux ans en arrière, sauf si l'utilisateur final a indiqué ne pas vouloir conserver cet historique.

La communication de ces données de l'environnement numérique de la bibliothèque vers le système de bibliothèque unifié est nécessaire pour permettre le fonctionnement du système et ainsi garantir un fonctionnement performant de la bibliothèque et une bonne gestion des emprunteurs (y compris la prise de contact et la communication avec les membres de la bibliothèque et la gestion des abonnements et des prêts) (voir également les finalités mentionnées au point 5.2 ci-dessous). Les finalités du traitement (voir également 5.2) ne peuvent raisonnablement être atteintes d'une autre manière.

Les données communiquées sont conservées pendant deux ans maximum après la fin de l'adhésion à la bibliothèque. Après la fin de l'abonnement et à condition qu'il n'y ait pas de transactions et de frais en suspens, ce délai de conservation commence à courir et, à son expiration, les données sont automatiquement supprimées du système. Si une bibliothèque n'est plus affiliée au système de bibliothèque unifié, les données à caractère personnel de ses membres sont supprimées, conformément aux dispositions prévues dans la convention.

5.2 Finalités et base juridique

Les finalités pour lesquelles les données ont été initialement collectées par les bibliothèques/communes et pour lesquelles elles sont communiquées à Cultuurconnect lors de leur raccordement au système bibliothécaire unifié sont les suivantes :

- À des fins d'identification et d'autorisation
    - traitements dans le cadre de l'identification et de l'autorisation des utilisateurs finaux ;
- Finalités de gestion
    - traitements dans le cadre de l'exploitation et de la gestion : les employés de bibliothèque habilités ont accès au système de bibliothèque afin de l'exploiter et de le gérer, par exemple pour inscrire un client, rechercher un client afin de lui prêter un exemplaire, dédupliquer un client qui apparaît deux fois dans le système, etc.
    - traitements dans le cadre de la gestion et du service d'assistance ;
    - traitements dans le cadre du développement, de l'hébergement, du support et du service d'assistance par les employés autorisés du fournisseur informatique.
- Finalités fonctionnelles, entre autres
    - traitements dans le cadre de la détermination du type d'abonnement ;
    - traitements dans le cadre du suivi des soldes impayés ;
    - traitements dans le cadre de l'envoi d'e-mails de rappel, de rappels, de messages de réservation.
- Finalités liées à l'échange de données, notamment
    - traitements dans le cadre de la connexion entre Ma Bibliothèque et le système de bibliothèque en fonction des services en ligne de la bibliothèque pour l'utilisateur final ;
    - traitements dans le cadre de la connexion entre le système de bibliothèque et le registre national afin de garantir l'exactitude et l'actualité des données de l'utilisateur final.
- Finalités de la journalisation
    - traitements dans le cadre de l'enregistrement des activités des utilisateurs à des fins de résolution de problèmes et d'audit ;

    - traitements dans le cadre de l'enregistrement et du suivi des opérations effectuées par les administrateurs sur les données à caractère personnel.
- Finalités de communication et de marketing direct
    - traitements dans le cadre de la communication sur les activités et les services de la bibliothèque.
- Finalités statistiques
    - traitements dans le cadre de la génération de rapports et de statistiques basés sur l'utilisation du point de vue de la bibliothèque.

La collecte et le traitement des données à caractère personnel à ces fins sont effectués sur la base de l'accord conclu entre la bibliothèque et l'utilisateur final lors de l'adhésion à la bibliothèque. Le traitement par Cultuurconnect des données communiquées est effectué aux mêmes fins.

Cultuurconnect traite les données à caractère personnel communiquées à des fins supplémentaires :

- Finalités de l'échange de données
    - traitements dans le cadre de développements futurs et de liens en fonction d'objectifs culturels supralocaux et de la poursuite de l'innovation de la politique culturelle locale (voir 4.6 ci-dessus) ;
- Finalités de communication et de marketing direct
    - traitements dans le cadre de la communication et du marketing direct dans une perspective supralocale en rapport avec les services utilisés et les applications disponibles ;
- Finalités statistiques
    - traitements dans le cadre de la génération de rapports et de statistiques sur la base de l'utilisation dans une perspective supralocale.

Ces objectifs sont compatibles avec les objectifs initiaux :

- Les utilisateurs finaux, les bibliothèques, la VGC et Cultuurconnect ont tout intérêt à ce que l'infrastructure de base de la bibliothèque numérique soit efficace, pertinente et mise à jour conformément aux modalités mentionnées au point 4.6, afin de pouvoir continuer à réaliser l'objectif de l'infrastructure de base (voir ci-dessus, 1). En ce sens, les traitements effectués dans ce cadre sont également dans l'intérêt légitime de Cultuurconnect en tant qu'organisateur de l'infrastructure de base.
- L'envoi de communications et de marketing direct aux utilisateurs finaux en rapport avec les produits et services disponibles via l'infrastructure de base de la bibliothèque numérique pour les utilisateurs finaux concernés fait partie des attentes raisonnables des utilisateurs finaux des produits et services de bibliothèque. Dans tous les cas, Cultuurconnect prend des mesures pour informer les utilisateurs finaux à ce sujet et sur leur droit de s'y opposer (notamment par le biais d'une déclaration de confidentialité), et chaque communication prévoit une possibilité effective de désinscription, qui entraîne la suppression de la liste sur la base de laquelle la communication est envoyée (article XII.13 du Code de droit économique).
- Le traitement ultérieur à des fins statistiques est un traitement compatible avec les finalités initiales (voir l'article 89 du RGPD ; voir également la

loi sur la protection des données du 30 juillet 2018). Dans tous les cas, Cultuurconnect prend des mesures pour informer les utilisateurs finaux à ce sujet et sur leur droit de s'y opposer (notamment par le biais d'une déclaration de confidentialité), et ce traitement à des fins statistiques est effectué de manière pseudonymisée.

PARTIE 2 : UTILISATION DES DONNÉES

1. Utilisation et traitement autorisés des données à caractère personnel d'

Les collaborateurs compétents de la VGC sont autorisés, dans le cadre de l'objet du Contrat et dans le respect des dispositions du présent règlement d'utilisation, à accéder aux données à caractère personnel des utilisateurs finaux et à effectuer des actions sur ces données dans le cadre :

- l'exploitation et la gestion du système de bibliothèque (par exemple, inscrire un client, rechercher un client pour lui prêter un exemplaire, dédupliquer un client qui apparaît deux fois dans le système, etc.) ;
- l'interface et la gestion du contenu dans le cadre du site web de la bibliothèque ;
- la gestion des utilisateurs des profils « Ma bibliothèque ».

Cultuurconnect prend les mesures techniques nécessaires pour garantir que :

- les collaborateurs compétents de la VGC aient uniquement accès aux données de leurs propres utilisateurs finaux, c'est-à-dire les utilisateurs finaux qui sont abonnés aux bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale.
- Les employés compétents des bibliothèques publiques néerlandophones des communes affiliées ont uniquement accès aux données de leurs propres utilisateurs finaux, c'est-à-dire les utilisateurs finaux qui ont un abonnement auprès de leur propre bibliothèque ou groupe de coopération.
- Lors de l'inscription d'un nouvel utilisateur final, un doublon est suggéré si la personne figure déjà dans le système. La commune/bibliothèque peut alors ajouter un abonnement à cette personne ;
- Les employés autorisés de la VGC ont uniquement accès aux profils « Ma bibliothèque » des utilisateurs finaux des bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale.
- Les employés autorisés des bibliothèques publiques néerlandophones des communes affiliées ont uniquement accès aux profils « Ma bibliothèque » des utilisateurs finaux de leur propre bibliothèque.

2. Obligations de l'

2.1 Généralités

Dans le cadre de l'exécution des tâches liées à sa participation à l'infrastructure de base de la bibliothèque numérique, la VGC traitera (utilisera, modifiera, stockera, etc.) les données à caractère personnel des utilisateurs finaux pendant toute la durée de la participation, conformément à la législation applicable en matière de protection des données.

2.2 Responsabilité vis-à-vis de ses propres collaborateurs

La VGC est responsable de la conformité de ses propres collaborateurs ou mandataires avec le RGPD, de la manière dont ils introduisent les données à caractère personnel dans le système bibliothécaire et des actions qu'ils entreprennent sur les données à caractère personnel auxquelles ils ont accès. Cette responsabilité et cette obligation comprennent également le respect des dispositions de l'accord et de la présente annexe, ainsi que le respect des lois et réglementations applicables. Cultuurconnect n'assume donc aucune responsabilité quant aux actions ou omissions des employés ou mandataires de la VGC.

Dans le cadre de l'utilisation autorisée, la VGC prévoit des mesures organisationnelles appropriées pour protéger les données à caractère personnel et garantir leur fiabilité, leur disponibilité et leur intégrité. Sans que cela ait un effet limitatif, la VGC garantit au moins les mesures suivantes :

- Seuls les collaborateurs habilités de la VGC peuvent avoir accès aux données à caractère personnel. La VGC est au moins responsable de déterminer les compétences des collaborateurs, de suivre et de contrôler le respect de celles-ci, et de respecter le principe du besoin d'en connaître à l'égard des collaborateurs.

- Les collaborateurs compétents de la VGC reçoivent un identifiant personnel avec un rôle d'utilisateur spécifique. Le rôle utilisateur d'un collaborateur détermine les données auxquelles il a accès. Les rôles utilisateurs et les droits (d'accès) qui y sont associés sont documentés en détail dans le manuel. Il incombe à la VGC de demander le rôle utilisateur approprié pour le collaborateur et de signaler le départ d'un collaborateur. Le service d'assistance Cultuurconnect supprime alors l'identifiant de l'employé.

- Les collaborateurs peuvent modifier eux-mêmes leur mot de passe et doivent le faire régulièrement, le système imposant un mot de passe fort. À terme, il est prévu de rendre l'expiration du mot de passe configurable pour le système.

- L'accès au compte personnel doit être suffisamment protégé, notamment en se déconnectant de l'application en temps utile. Il est recommandé à la VGC de mettre en place un verrouillage au niveau du système d'exploitation.

- La VGC veille à ce que chaque collaborateur ou mandataire compétent soit informé/formé de manière actualisée sur ses obligations et responsabilités en matière de sécurité de l'information et de confidentialité des données à caractère personnel. La VGC oblige ses propres collaborateurs à n'accéder aux données à caractère personnel que dans le cadre strict de l'exercice de leurs fonctions (par exemple, par une déclaration sur l'honneur ou par l'intégration dans le règlement de travail ou le contrat de travail) et applique à tous ses collaborateurs une politique interdisant la divulgation d'informations confidentielles.

- Les champs de texte libre dans le logiciel (tels que les champs « commentaires ») ne sont pas conçus pour le traitement de données à caractère personnel. La VGC veille à ce qu'aucune donnée à caractère personnel ne soit saisie dans ces champs.

- L'infrastructure de base de la bibliothèque numérique n'exige en aucun cas le stockage hors ligne de données à caractère personnel. Tout stockage hors ligne relève donc de la responsabilité exclusive de la VGC.

2.3 Communication à partir du système de bibliothèque

2.3.1 Communication fonctionnelle

Le système de bibliothèque envoie des courriels qui font partie des processus administratifs de la bibliothèque, par exemple lorsqu'une réservation est prête, lorsque des documents empruntés ne sont pas rendus à temps, des courriels de pénalité,...Ces e-mails sont envoyés par défaut si l'emprunteur
a communiqué une adresse e-mail au guichet ou est enregistré dans Ma bibliothèque. Si aucune adresse e-mail n'a été communiquée, ces messages sont envoyés par courrier postal. Les utilisateurs finaux ne peuvent pas choisir de ne pas recevoir ces messages, car ils sont fonctionnels et nécessaires aux processus de travail au sein de la bibliothèque.

Les rappels de retour constituent une catégorie à part. Il s'agit d'e-mails envoyés par le système de la bibliothèque quelques jours avant l'expiration du délai de prêt. Ces « e-mails de rappel » sont plutôt un service de confort et peuvent être désactivés par l'utilisateur final. Cette option est disponible en tant qu'opt-in dans le client, de sorte qu'un employé autorisé peut l'activer ou la désactiver à la demande d'un utilisateur final. La commune/bibliothèque est donc responsable de la gestion des utilisateurs de la fonctionnalité « rappels de retour » à la demande de l'utilisateur final. À terme, il est prévu d'intégrer l'option opt-in dans Ma Bibliothèque, afin que l'utilisateur final puisse gérer lui-même ses autorisations à tout moment via Ma Bibliothèque.

2.3.2 Module marketing

Les bibliothèques peuvent également utiliser le module marketing du système bibliothécaire pour envoyer des newsletters, des campagnes, etc. à leurs membres. Ce module marketing sera à terme aménagé plus en détail, avec des options disponibles en opt-in dans le client, et en accordant une attention particulière aux possibilités pour l'utilisateur final de gérer lui-même son consentement à recevoir de telles communications via le profil Ma bibliothèque. Si la commune/bibliothèque utilise le module marketing, elle est alors responsable du contenu des communications envoyées de cette manière et de la gestion des utilisateurs de cette fonctionnalité à la demande de l'utilisateur final.

2.4 Rapports et statistiques

Les collaborateurs compétents de la VGC peuvent générer et consulter des rapports et des statistiques sur l'utilisation de certaines applications par les utilisateurs finaux des bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale dans le cadre d'un traitement statistique pseudonymisé (par exemple, nombre de renouvellements à la bibliothèque, sexe et âge, utilisation, utilisation des collections numériques, ...).

Les collaborateurs compétents des bibliothèques publiques néerlandophones des communes affiliées peuvent générer et consulter des rapports et des statistiques sur l'utilisation de certaines applications par leurs propres utilisateurs finaux dans le cadre d'un traitement statistique pseudonymisé (par exemple, nombre de prolongations à la bibliothèque, sexe et âge, utilisation, utilisation des collections numériques, ...).

2.5 Fourniture d'informations aux utilisateurs finaux

Cultuurconnect a élaboré une déclaration de confidentialité relative à l'infrastructure de base de la bibliothèque numérique.

La VGC s'engage, dans le cadre de sa relation contractuelle avec les communes bruxelloises, à prévoir une méthode de travail afin que la déclaration de confidentialité relative à l'infrastructure de base de la bibliothèque numérique, ainsi que toute modification future de celle-ci discutée avec le groupe de pilotage de l'infrastructure de base de la bibliothèque numérique, soient intégrées dans les informations fournies aux utilisateurs finaux, une première fois à l'occasion de la participation à l'infrastructure de base de la bibliothèque numérique. Cette méthode de travail garantit que l'utilisateur final est informé de l'existence et du contenu de cette déclaration de confidentialité dans un délai raisonnable après le début de sa participation à l'infrastructure de base de la bibliothèque numérique et dans un délai raisonnable après la notification de toute modification de la déclaration de confidentialité. Cela peut se faire, par exemple, par l'intégration dans le règlement de la bibliothèque, ou par la remise d'une brochure illustrant les informations actuelles de la déclaration de confidentialité pour l'utilisateur final. La bibliothèque/commune veille à ce qu'une copie de la déclaration de confidentialité de l'infrastructure de base de la bibliothèque numérique (dans sa version la plus récente) soit toujours disponible à chaque comptoir de la bibliothèque.

La déclaration de confidentialité relative à l'infrastructure de base de la bibliothèque numérique est également publiée par Cultuurconnect sur le site web de la bibliothèque. La VGC, respectivement la commune/bibliothèque, s'engage à ne pas publier sur son propre site web de bibliothèque des déclarations supplémentaires qui contiendraient des informations contradictoires par rapport à la déclaration de confidentialité relative à l'infrastructure de base de la bibliothèque numérique. Chaque fois que la Déclaration de confidentialité relative à l'infrastructure de base de la bibliothèque numérique est modifiée, l'utilisateur final en est informé lors de sa prochaine connexion à Ma bibliothèque.

2.6 Assistance en cas de fuites de données

Si la VGC constate une fuite de données, elle en informera Cultuurconnect dans les plus brefs délais. Il y a fuite de données lorsque des données à caractère personnel sont divulguées, perdues, détruites ou modifiées de manière illicite.

Si une fuite de données est soumise à une obligation légale de notification, Cultuurconnect décidera, en fonction de la situation concrète, s'il convient que la notification soit effectuée par Cultuurconnect, par chaque commune/bibliothèque auprès de ses utilisateurs finaux concernés, ou par la VGC. Dans ce dernier cas, la commune/bibliothèque ou la VGC s'engage à effectuer la notification selon les modalités (contenu, timing) communiquées par Cultuurconnect.

La communication entre Cultuurconnect et la VGC à ce sujet se fait en principe entre les personnes de contact mentionnées dans la partie 1, 4.7.2.

2.7 Assistance en cas de demandes de l'Autorité de contrôle

Si une demande, une communication, un avis ou une injonction de l'Autorité de contrôle parvient directement à la VGC, celle-ci en informera immédiatement Cultuurconnect, au plus tard dans les cinq jours ouvrables.

La VGC apporte, sur demande, une assistance raisonnable à Cultuurconnect pour répondre à une demande, une communication, un avis ou une injonction de l'Autorité de contrôle.

La communication entre Cultuurconnect et la VGC à ce sujet se fait en principe entre les délégués à la protection des données mentionnés dans la partie 1, 4.7.1.

2.8 Assistance en cas de demandes des personnes concernées

Si une demande émanant d'une personne concernée est adressée directement à la commune/bibliothèque ou à la VGC, celle-ci s'efforcera dans un premier temps de donner suite aux demandes des personnes concernées qui prouvent leur identité. Dans ce cas, Cultuurconnect apportera son soutien si nécessaire.

S'il n'est pas possible ou souhaitable pour la commune/bibliothèque ou la VGC de donner suite elle-même aux demandes des personnes concernées, la commune/bibliothèque ou la VGC transmettra immédiatement, et au plus tard dans les cinq jours ouvrables, une copie de cette demande à Cultuurconnect.

La commune/bibliothèque ou la VGC apporte son aide à Cultuurconnect pour répondre aux demandes, si nécessaire, même si celles-ci sont adressées directement à Cultuurconnect.

Si Cultuurconnect ne reçoit pas de copie d'une demande de la commune/bibliothèque ou de la VGC, elle part du principe que la commune/bibliothèque ou la VGC traitera la demande en question dans les délais et de manière correcte. Dans ce cas, la responsabilité incombe à la commune/bibliothèque ou à la VGC.

3. Contrôle

Il incombe à toutes les parties prenantes de garantir au maximum l'intégrité de l'infrastructure de base de la bibliothèque numérique. La VGC, respectivement la commune/bibliothèque, s'engage à prendre des mesures raisonnables du point de vue de la protection de la vie privée afin de garantir, d'une part, le respect des dispositions du présent contrat d'utilisation des données par ses collaborateurs et, d'autre part, le comportement correct des utilisateurs finaux dans les bibliothèques.

Cultuurconnect surveille de manière active et réactive le respect de la présente annexe. S'il existe des indices raisonnables laissant supposer que la commune/bibliothèque ou la VGC ne respecte pas ses obligations au titre de la présente annexe, Cultuurconnect obtient un droit d'audit sur les activités de traitement et les installations de traitement de la commune/bibliothèque ou de la VGC. À cette fin, elle a le droit de se rendre, par l'intermédiaire d'un auditeur indépendant, dans les locaux ou les lieux où la commune/bibliothèque ou la VGC effectue le traitement des données, moyennant un préavis.

délai de préavis de deux semaines. La commune/bibliothèque, respectivement la VGC, apporte à cet égard une coopération raisonnable et fournira les informations nécessaires afin de permettre à l'auditeur d'évaluer si la commune/bibliothèque, respectivement la VGC, a respecté ses obligations au titre de la présente annexe. Les frais d'un tel audit sont à la charge de Cultuurconnect. Si un manquement à la présente annexe de la part de la commune/bibliothèque ou de la VGC est constaté, Cultuurconnect et la VGC ou la commune/bibliothèque se concerter à ce sujet, en vue de trouver une solution dans un délai raisonnable, afin de ne pas compromettre l'utilisation de la VGC, respectivement de la commune/bibliothèque, dans le cadre de la présente annexe et la participation à l'infrastructure de base de la bibliothèque numérique. Le non-respect persistant des obligations de la présente annexe peut entraîner le refus d'accès à l'infrastructure de base de la bibliothèque numérique par la VGC ou la commune/bibliothèque.

PARTIE 3 : HORS DU CHAMP D'APPLICATION DE L'

1. ing direct personnalisé

Si la VGC souhaite envoyer des communications (par exemple sur ses propres activités et services) sur la base d'une liste d'adresses (électroniques) des utilisateurs finaux des bibliothèques publiques néerlandophones des communes affiliées à la Région de Bruxelles-Capitale, obtenue à partir de l'infrastructure de base de la bibliothèque numérique, la responsabilité en incombe (y compris le respect de la législation en vigueur en la matière ; traitement et protection des données à caractère personnel) incombe entièrement à la VGC en tant que responsable du traitement.

Si les communes affiliées de la Région de Bruxelles-Capitale souhaitent envoyer des communications (par exemple sur les activités et les services de leur propre bibliothèque) sur la base d'une liste d'adresses (électroniques) des utilisateurs finaux (utilisateurs finaux abonnés à leur propre bibliothèque ou à un partenariat) obtenue à partir de l'infrastructure de base de la bibliothèque numérique, la responsabilité en incombe (y compris le respect de la législation en vigueur en la matière ; traitement et protection des données à caractère personnel) incombe entièrement à la commune en tant que responsable du traitement.

La VGC ou la commune concernée est responsable de la base juridique du traitement et il lui incombe d'informer l'utilisateur final du traitement et de la protection de ses données à caractère personnel dans ce cadre.

2. Traitement propre en tant que responsable du traitement en dehors du cadre de l' t de l'infrastructure de base de la bibliothèque numérique

Si la VGC ou la commune affiliée de la Région de Bruxelles-Capitale souhaite enregistrer les données à caractère personnel des utilisateurs finaux des bibliothèques publiques néerlandophones des communes affiliées de la Région de Bruxelles-Capitale, respectivement ses propres utilisateurs finaux, provenant de l'infrastructure de base de la bibliothèque numérique dans d'autres systèmes, ou souhaite établir un lien avec d'autres systèmes ayant un impact sur ces données à caractère personnel, cela se fait sous l'entière responsabilité de la VGC ou de la commune concernée (y compris le respect de la législation en vigueur en la matière ; la création, la gestion et le paiement du compte de gestion de ses propres employés, y compris le

traitement des données à caractère personnel dans ce cadre). La VGC ou la commune concernée s'engage à ne procéder à tout moment qu'à un traitement complémentaire et propre des données à caractère personnel, à condition qu'il existe une base légale à cet effet, et à appliquer toutes les garanties prévues par la réglementation en matière de protection de la vie privée et, en particulier, le règlement général sur la protection des données (RGPD).

Les éléments ci-dessous (liste non exhaustive) ne relèvent en aucun cas du champ d'application de l'accord et de la présente annexe. Les traitements effectués dans ce cadre ne relèvent donc pas de la responsabilité de Cultuurconnect dans le cadre de l'infrastructure de base de la bibliothèque numérique. La VGC, respectivement la commune concernée, respecte toutes les obligations prévues par le RGPD à cet égard, y compris dans ses relations avec ses éventuels sous-traitants :

- Ajouter du contenu ou intégrer des médias sociaux dans le site web de la bibliothèque ;
- Fournir des services supplémentaires via le site web de la bibliothèque, tels qu'une application de newsletter, le paiement en ligne, etc.
- Liens/applications que la VGC, respectivement la commune concernée, construit elle-même sur les API Cultuurconnect (voir également l'article 6.4 de l'accord) ;
- La connexion et la sécurisation des communications entre les bibliothèques locales et les serveurs centraux ;
- Le réseau interbibliothèques local, c'est-à-dire la connexion entre la bibliothèque centrale et les autres sites ;
- Le réseau local de la bibliothèque, c'est-à-dire le réseau au sein de la bibliothèque principale et/ou de la succursale ou du point de prêt ;
- Le matériel informatique local (ordinateurs, scanners, imprimantes, routeurs, etc.) ;
- La connexion Internet vers les postes de travail destinés au public ;
- Toutes les applications bureautiques et autres qui ne font pas partie de l'infrastructure numérique de base, y compris (la connexion avec) les distributeurs automatiques locaux, tels que les appareils RFID et SIP2 locaux.

Cultuurconnect n'assume aucune responsabilité quant au traitement des données à caractère personnel dans ce contexte.